IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

ERICA TIERNEY, ANDRIS STRAUTINS, NATALIE ROBLES, JEFFREY BENKLER, ERICK D. OLIVER, and LILI ROBINSON, individually and on behalf of all others similarly situated,	
Plaintiffs,	**Case No: 1:13-cv-06237**
v.	
ADVOCATE HEALTH AND HOSPITALS CORP. a/k/a ADVOCATE MEDICAL GROUP, an Illinois corporation,	**JURY TRIAL DEMANDED**
Defendant.	

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Erica Tierney, Andris Strautins, Natalie Robles, Jeffrey Benkler, Erick D. Oliver, and Lili Robinson (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, by and through their attorneys, bring this action against Advocate Health and Hospitals Corp., a/k/a Advocate Medical Group ("Advocate" or "Defendant"), and hereby allege as follows:

NATURE OF THE CASE

1. This is a national consumer class action lawsuit brought by Plaintiffs, individually and on behalf of all other similarly situated persons (*i.e.*, the Class Members), whose personally identifiable information and personal health information (collectively referred to as "PII/PHI") entrusted to Advocate was stolen by a thief or thieves while in the possession, custody, and control of Advocate.

2. PII/PHI includes Plaintiffs' and Class Members' names, addresses, dates of birth, Social Security numbers, treating physician and/or departments for each individual, their medical diagnoses, medical record numbers, medical service codes, and health insurance information.

3. On July 15, 2013, four desktop computers containing the PII/PHI of Plaintiffs and more than four million Class Members were taken from an Advocate office located at 205 West Touhy, Park Ridge, Illinois (the "Data Breach").

4. Advocate flagrantly disregarded Plaintiffs' and Class Members' privacy rights by intentionally, willfully, recklessly, and/or negligently failing to take the necessary precautions required to safeguard and protect their PII/PHI from unauthorized disclosure. Plaintiffs' and Class Members' PII/PHI was improperly handled and stored, was unsecured, was unencrypted, and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiffs' and Class Members' PII/PHI was compromised and stolen.

5. Advocate's intentional, willful, reckless, and/or negligent disregard of Plaintiffs' and Class Members' rights directly and proximately caused the unauthorized disclosure of Plaintiffs' and Class Members' PII/PHI. The improper use of PII/PHI by unauthorized third parties can have and has had a serious adverse impact on, among other things, a victim's credit rating and finances. The type of wrongful PII/PHI disclosure made by Advocate is of the most harmful because it generally takes a significant amount of time for a victim to become aware of misuse of that PII/PHI.

6. On behalf of themselves and Class Members, Plaintiffs have standing to bring this lawsuit because their PII/PHI was included in the Data Breach and they were damaged as a direct and proximate result of Advocate's wrongful actions and inaction and the resulting Data Breach.

7. Advocate's wrongful actions and inaction and the resulting Data Breach have, *inter alia*, placed Plaintiffs and Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[1] Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released a 2012 Identity Fraud Report (the "Javelin Report"), quantifying the impact of data breaches. According to the Javelin Report, individuals whose PII/PHI is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity theft and/or identity fraud has not yet been discovered or reported and a high probability that criminals who may now possess Plaintiffs' and Class Members' PII/PHI have not yet used the information but will do so later, or re-sell it. Even without such loss, Plaintiffs and Class Members are entitled to relief and recovery, including statutory damages under federal statutory provisions, as set forth herein.

8. Advocate's failure to safeguard and protect Plaintiffs' and Class Members' PII/PHI violated the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* ("FCRA"). Advocate failed to adopt, implement, and maintain adequate procedures to protect such information and to limit the dissemination of same to the permissible purposes under FCRA. In further violation of FCRA, Advocate failed to protect and wrongfully disseminated Plaintiffs' and Class Members' PII/PHI, which is "medical information" specifically protected by FCRA. As a direct and proximate result of Advocate's willful, reckless, and/or grossly negligent

[1] According to the United States Government Accounting Office ("GAO"), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities, such as when PII/PHI is used to commit fraud or other crimes (credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services)).

violations of FCRA, an unauthorized third party (or parties) obtained Plaintiffs' and Class Members' PII/PHI for no permissible purpose under FCRA.

9. Advocate's wrongful actions and inaction and the resulting Data Breach also constitute common law negligence and common law invasion of privacy by public disclosure of private facts.

10. Plaintiffs, on behalf of themselves and the Class Members, seek actual damages, economic damages, statutory damages, nominal damages, exemplary damages, injunctive relief, attorneys' fees, litigation expenses and costs of suit.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over Plaintiffs' FCRA claims pursuant to 28 U.S.C. § 1331 (federal question). This Court also has subject matter jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367. This Court has personal jurisdiction over Advocate because at all relevant times, Advocate conducted (and continues to conduct) substantial business in the Northern District of Illinois.

12. Venue is proper in the Northern District of Illinois pursuant to 28 U.S.C. § 1391(b) and (c), because a substantial part, if not all, of the events giving rise to this action occurred in the Northern District of Illinois and Advocate resides, is located, can be found, and conducts substantial business in the Northern District of Illinois.

PARTIES

Plaintiff Erica Tierney

13. Plaintiff Erica Tierney ("Tierney") is an Illinois citizen residing in the Northern District of Illinois. Tierney was treated at one of Advocate's facilities in Illinois during the

relevant time period. On August 28, 2013, Tierney was advised that her PII/PHI was on the desktop computers stolen and compromised in the Data Breach.

14. Tierney's PII/PHI, which she entrusted to Advocate and which Advocate failed to properly safeguard and protect, was stolen from Advocate on July 15, 2013.

15. As a direct and proximate result of Advocate's wrongful actions and inaction and the resulting Data Breach, Tierney has suffered (and will continue to suffer) economic damages and other actual harm, including, but not limited to, emotional distress over learning of the theft of her PII/PHI, the general inconvenience and annoyance of dealing with her stolen, compromised and disseminated PII/PHI, and statutory damages under FCRA. Advocate's wrongful disclosure of and failure to safeguard and protect Tierney's PII/PHI has also placed her at an imminent, immediate, and continuing increased risk of harm from identity theft, identity fraud, and medical fraud.

Plaintiff Andris Strautins

16. Plaintiff Andris Strautins ("Strautins") is an Illinois citizen residing in the Northern District of Illinois. Strautins was treated at one of Advocate's facilities in Illinois during the relevant time period. On or about August 26, 2013, Strautins received a letter from Advocate advising him that his PII/PHI was on the desktop computers stolen and compromised in the Data Breach.

17. Strautins' PII/PHI, which he entrusted to Advocate and which Advocate failed to properly safeguard and protect, was stolen from Advocate on July 15, 2013.

18. As a direct and proximate result of Advocate's wrongful actions and inaction and the resulting Data Breach, Strautins has suffered (and will continue to suffer) economic damages and other actual harm, including, but not limited to, anxiety over learning of the theft of his

PII/PHI, the general inconvenience and annoyance of dealing with his stolen, compromised and disseminated PII/PHI, and statutory damages under FCRA. Advocate's wrongful disclosure of and failure to safeguard and protect Strautins' PII/PHI has also placed him at an imminent, immediate, and continuing increased risk of harm from identity theft, identity fraud, and medical fraud.

Plaintiff Natalie Robles

19. Plaintiff Natalie Robles ("Robles") is an Illinois citizen residing in the Northern District of Illinois. Robles was treated at one of Advocate's facilities in Illinois during the relevant time period. In August 2013, Robles was advised that her PII/PHI was on the desktop computers stolen and compromised in the Data Breach.

20. Robles's PII/PHI, which she entrusted to Advocate and which Advocate failed to properly safeguard and protect, was stolen from Advocate on July 15, 2013.

21. As a direct and proximate result of Advocate's wrongful actions and inaction and the resulting Data Breach, Robles has suffered (and will continue to suffer) economic damages and other actual harm, including, but not limited to, the general inconvenience and annoyance of dealing with her stolen, compromised and disseminated PII/PHI, and statutory damages under FCRA. Advocate's wrongful disclosure of and failure to safeguard Robles's PII/PHI has also placed her at an imminent, immediate, and continuing increased risk of harm from identity theft, identity fraud, and medical fraud.

Plaintiff Jeffrey Benkler

22. Plaintiff Jeffrey Benkler ("Benkler") is an Illinois citizen residing in the Northern District of Illinois. Benkler was treated at one of Advocate's facilities in Illinois during the

relevant time period. In late August 2013, Benkler was advised by Advocate that his PII/PHI was on the desktop computers stolen and compromised in the Data Breach.

23. Benkler's PII/PHI, which he entrusted to Advocate and which Advocate failed to properly safeguard and protect, was stolen from Advocate on July 15, 2013.

24. Benkler is an engineer. He and his wife also operate a customs brokerage business. The Benklers are meticulous protectors of their business and personal PII/PHI, regularly shredding receipts, statements and other documents containing their PII/PHI. The Benklers have never been victims of a PII or PHI data breach other than the Advocate Data Breach.

25. The Benklers maintain their personal and business bank accounts at a Chicago area branch of Citibank. On October 31, 2013, shortly after the Data Breach occurred, Benkler received a telephone call from the Citibank customer call center notifying him that someone was attempting to access his personal bank accounts. As a result, Citibank froze his accounts and cancelled his debit card.

26. Thereafter on October 31, 2013, Benkler spent two hours making the five mile roundtrip to the Chicago Citibank branch to secure his new debit card, place fraud alerts on his accounts, and meet with bank personnel to discuss various options to secure his financial accounts and information.

27. On November 1, 2013, and notwithstanding the time and effort he spent securing his financial accounts and information on October 31, Benkler received a telephone call from a Citibank branch manager in Philadelphia, Pennsylvania, informing him that a man claiming to be Benkler was in the bank attempting to secure a debit card for Benkler's personal checking account.

28. When Benkler properly confirmed his identity to the Philadelphia Citibank branch manager, the manager immediately ordered bank security personnel to arrest the imposter. Benkler heard the ensuing melee at the bank while on the telephone with the branch manager.

29. The arrested imposter had multiple identities on his person (fraudulent personal identification cards), including one identifying himself as Benkler which, on information and belief, the imposter purchased on the black market.

30. Benkler spent his entire November 1 workday afternoon speaking with Citibank personnel at the Chicago branch bank and the Philadelphia branch bank, Citibank corporate fraud personnel, and the Philadelphia police regarding the October 31 and November 1 attempts to access his financial accounts and information and how to best protect the financial accounts and information going forward.

31. Thereafter, on November 2, 2013, Benkler spent another two hours making the five mile return roundtrip to the Chicago Citibank branch to take additional steps to secure his financial accounts and information.

32. After the second trip to the Chicago Citibank branch, Benkler spent another five hours working online to coordinate other financial transactions impacted by closing his primary checking account and opening a new primary checking account, such as credit card auto-pay, automated bill payments, and payroll direct deposits. Even then, the credit card auto-pay adjustments went badly; to wit, short notice caused the auto-pays to miss a cycle which, in turn, resulted in late fee assessments, which, in turn, required an additional time investment to contact the credit card companies to secure refunds of the late fees. As of the time this Amended Consolidated Complaint was filed, Benkler was still dealing with automatic investments attempting to draw from his closed accounts.

33. In addition, the Citigroup home equity line of credit the Benklers use to operate their customs brokerage business was frozen. Benkler could not access the home equity line of credit during November, which required the Benklers to harass their customers for early payment so they could meet their obligations to United States Customs—which strained their client relationships. There also was no online access between the Benklers' business and personal accounts—which further strained their business and personal financial resources and placed Benkler's wife in a perilous management situation while Benkler was out of the country and largely unreachable.

34. All of the above-described incidents were the direct and proximate result of the Data Breach. As a direct and proximate result of Advocate's wrongful actions and inaction and the resulting Data Breach, Benkler's PII/PHI was stolen, compromised and disseminated to the world, for which he incurred and will continue to incur damages in the form of, *inter alia*, (i) lost time (a) driving to the Chicago Citibank branch to obtain the replacement debit card and secure their financial accounts and information, (b) dealing with Citibank personnel at the Chicago branch bank and the Philadelphia branch bank, Citibank corporate fraud personnel, and the Philadelphia police regarding the imposter, (c) generally securing his financial accounts and information, and (d) coordinating other financial transactions impacted by closing his primary checking account and opening a new primary checking account (for a total of at least 11 hours at $60/per hour = $660); (ii) mileage and other out of pocket expenses pertaining to (i), above; (iii) the lost value of his PII/PHI which, on information and belief, was sold to the imposter on the black market; (iv) strained relations with the Benklers' customs brokerage business customers because they could not access their home equity line of credit; (v) the inconvenience and annoyance of dealing with their stolen, compromised and disseminated PII/PHI; and (vi)

statutory damages under FCRA. Advocate's wrongful disclosure of, and failure to safeguard and protect, Benkler's PII/PHI has also placed him at an imminent, immediate, and continuing increased risk of harm from identity theft, identity fraud, and medical fraud (in addition to the attempts he already has experienced).

Plaintiff Erick D. Oliver

35. Plaintiff Erick D. Oliver ("Oliver") is an Illinois citizen residing in the Northern District of Illinois. Oliver was treated at one of Advocate's facilities in Illinois during the relevant time period. On or about August 23, 2013, Oliver received a letter from Advocate advising him that his PII/PHI was on the desktop computers stolen and compromised in the Data Breach.

36. Oliver's PII/PHI, which he entrusted to Advocate and which Advocate failed to properly safeguard and protect, was stolen from Advocate on July 15, 2013.

37. On or about September 18, 2013, Oliver was notified that one or more individuals had opened cell phone accounts in his name with Verizon and AT&T. Regarding the Verizon account, approximately $635.00 of charges were made in Oliver's name, which were billed to Oliver by Verizon. Regarding the AT&T account, five (5) cell phones were fraudulently purchased in Oliver's name, which Oliver learned of via a telephone call from AT&T's fraud department.

38. Oliver contacted both Verizon and AT&T to dispute the charges. AT&T removed the fraudulent charges from its system, but Verizon refused to do so without being provided a copy of a police report regarding the improper charges.

39. On September 28, 2013, Oliver filed a report with the Chicago Police Department, detailing the fraudulent Verizon charges and the Data Breach.

40. Oliver paid for a copy of the police report, which he provided to Verizon. Verizon subsequently removed the fraudulent charges from its system.

41. Oliver spent approximately 15 hours to correct the above-referenced fraudulent activity committed in his name, including substantial time spent on the phone, driving to the Chicago Police Department to file a police report, and sending and reviewing numerous electronic communications.

42. Oliver has not received a data breach notification—other than the Advocate data breach notification—informing him that his PII/PHI had been compromised.

43. As a direct and proximate result of Advocate's wrongful actions and inaction and the resulting Data Breach, Oliver has suffered (and will continue to suffer) economic damages and other actual harm, including, but not limited to, the general inconvenience and annoyance of dealing with his stolen, compromised and disseminated PII/PHI, and statutory damages under FCRA. Advocate's wrongful disclosure of, and failure to safeguard and protect Oliver's PII/PHI has already subjected Oliver to two (2) separate instances of identity fraud, and placed him at an imminent, immediate, and continuing increased risk of further harm from identity theft, identity fraud, and medical fraud.

Plaintiff Lili Robinson

44. Plaintiff Lili Robinson ("Robinson") is a Florida citizen residing in Florida. Robinson was treated at one of Advocate's facilities in Illinois during the relevant time period. Robinson called Advocate to determine whether her PII/PHI was on the desktop computers stolen and compromised in the Data Breach, and was advised by Advocate that her PII/PHI was on the stolen desktop computers. To date, however, Robinson has not received a formal data breach notification letter from Advocate.

45. Robinson's PII/PHI, which she entrusted to Advocate and which Advocate failed to properly safeguard and protect, was stolen from Advocate on July 15, 2013.

46. As a direct and proximate result of Advocate's wrongful actions and inaction and the resulting Data Breach, Robinson has suffered (and will continue to suffer) economic damages and other actual harm, including, but not limited to, the general inconvenience and annoyance of dealing with her stolen, compromised and disseminated PII/PHI, and statutory damages under FCRA. Advocate's wrongful disclosure of and failure to safeguard and protect Robinson's PII/PHI has also placed her at an imminent, immediate, and continuing increased risk of harm from identity theft, identity fraud, and medical fraud.

Advocate Health and Hospitals Corp.

47. Defendant Advocate Health and Hospitals Corp. a/k/a Advocate Medical Group is a network of affiliated doctors and hospitals that treat patients throughout Illinois, with its principal place of business in Downers Grove, Illinois.

48. Advocate has been recognized as one of the country's top 10 health systems, and is the largest integrated health care system in the state.

49. Advocate handles Plaintiffs' and Class Members' PII/PHI in numerous ways, including, *inter alia*: 1) maintaining the PII/PHI for its own files; and 2) submitting the PII/PHI to insurance companies and state and federal agencies for purposes of, *inter alia*, obtaining payment for health care services provided to its patients.

50. When communicating with insurance companies and state and federal agencies for purposes of obtaining payment for health care services that its physicians have rendered, Advocate assembles Plaintiffs' and Class Members' PII/PHI and transmits it to the insurance companies and state and federal agencies. The insurance companies and state and federal

agencies, in turn, utilize Plaintiffs' and Class Members' PII/PHI for a variety of purposes, including, *inter alia*, setting rates for health insurance, life insurance, and other types of insurance, and setting rates for the payment of certain health care services.

51. Advocate also assembles Plaintiffs' and Class Members' PII/PHI and transmits it to the insurance companies and state and federal agencies for purposes of determining whether Plaintiffs and Class Members are eligible for various medical treatments and the insurance coverage of such treatments.

52. Additionally, Advocate, through Advocate Physician Partners, collects, manages, and shares a multitude of patient information—including Plaintiffs' and Class Members' PII/PHI—in a variety of ways, including but not limited to:

a. Advocate's "nationally recognized Clinical Integration Program—a collaborative effort by more than 4,000 physicians and ten Advocate hospitals to drive improvements in health care quality and efficiency;"[2]

b. Advocate's Medicare Shared Savings Program, whereby Advocate "is able to impact the health of over 100,000 Medicare beneficiaries in the Chicagoland and Central Illinois regions. Along with attributed patients in Advocate's shared savings partnership with Blue Cross and Blue Shield of Illinois, these patients benefit[] from AdvocateCare, Advocate's accountable care program that aims to improve health outcomes, patient safety and the patient experience while providing care in a cost-effective manner;"[3]

c. Through Advocate's Medicare Shared Savings Program, Advocate has "one of the largest shared savings/risk populations under management in the country;"[4]

[2] http://www.advocatehealth.com/body.cfm?id=2744 (last visited Dec. 4, 2013).

[3] "The 2013 Value Report," Advocate Physician Partners, available at http://www.advocatehealth.com/documents/app/2013ValueReport-Complete.pdf (last visited Dec. 4, 2013).

[4] *Id.*

d. In 2011, Advocate entered into a shared savings contract with its biggest commercial insurance partner;[5]

e. Through Advocate assessing and sharing PII/PHI to reduce readmissions, better manage patients to avoid unnecessary admissions, and shorten lengths of stays, all through the use of "[s]ophisticated data systems[, which] are enabling greater abilities to work with patients in new ways to increase medical literacy, engage patients in shared decision making and help patients navigate the complex health care system;"[6] and

f. Through Advocate hiring "outpatient care managers dedicated to primary care offices to manage complex, high risk commercial and Medicare patients," and to help "identify and prioritize these patients, Advocate Physician Partners has invested in software that risk-stratifies patients using predictive modeling capabilities. Care managers work closely with the patient's primary care physician to identify and help address social, financial, educational and practical barriers to needed care."[7]

BACKGROUND FACTS

53. In the regular course of its business, Advocate collects and maintains possession, custody, and control of a wide variety of personal and confidential information, including Plaintiffs' and Class Members' PII/PHI.

54. Advocate stored Plaintiffs' and Class Members' PII/PHI, at a minimum, in an unencrypted format on four unsecured and unmonitored desktop computers, which is against industry practices and in violation of the Health Insurance Portability and Accountability Act of 1996.

55. Advocate has admitted that the PII/PHI was improperly stored: "Kelly Jo Golson, an Advocate senior vice president, acknowledged . . . that some of the data at risk qualifies as protected health information under the law. She also said the sensitive data should not have been

[5] *Id.*

[6] *Id.*

[7] *Id.*

stored on the computers' hard drives. 'This type of data should always be maintained on our secure network,' she said," and not on administrative computers, such as the desktop computers that were taken. [8]

56. Mac McMillan, CEO of the consulting firm CynergisTek, in commenting on the method of storage by Advocate, stated: "I have to shake my head when I see 4 million patient records on desktops. It defies common sense and logic." *Id.*

57. The unmonitored room in Advocate's administrative offices in Park Ridge, Illinois, where the unsecured computers containing Plaintiffs' and Class Members' unencrypted PII/PHI were stored, had no security to prevent unauthorized access.

58. Advocate does not know the whereabouts of the four desktop computers.[9]

59. According to Advocate, the desktop computers contain the unencrypted PII/PHI of Plaintiffs and approximately 4.03 million Class Members, all of whom are (or were) Advocate Health Care patients "seen by Advocate Medical Group physicians, either in a medical office or a hospital, from the early 1990s through July" 2013. [10]

60. The Data Breach is "the second-largest loss of unsecured protected health information reported to the Department of Health and Human Services since it implemented a mandatory notification rule in September 2009."[11]

---

[8] "Regulators to Investigate Advocate Data Breach," CHICAGO TRIBUNE (Aug. 28, 2013), available at http://articles.chicagotribune.com/2013-08-28/business/chi-advocate-20130828_1_medical-data-health-information-medical-record-numbers (last visited Dec. 4, 2013).

[9] "Advocate Medical Group Notifies Patients, Offers Protection Following Office Burglary," Advocate Health Care Press Release, available at http://www.advocatehealth.com/body_full.cfm?id=12&action=detail&ref=293 (last visited Dec. 4, 2013).

[10] "Regulators to Investigate Advocate Data Breach," CHICAGO TRIBUNE (Aug. 28, 2013), available at http://articles.chicagotribune.com/2013-08-28/business/chi-advocate-20130828_1_medical-data-health-information-medical-record-numbers (last visited Dec. 4, 2013).

[11] *Id.*

61. Despite knowing about the Data Breach since at least July 15, 2013, Advocate did not begin to formally notify Plaintiffs and Class Members of the Data Breach until August 23, 2013—more than one month after the theft of the four desktop computers.

62. During the intervening period between the Data Breach and the date the first wave of notification letters was sent to Plaintiffs and Class Members on August 23, 2013, their unencrypted PII/PHI could have been bought and sold several times on the robust international cyber black market while they had no chance whatsoever to take measures to protect their privacy.

63. The fact that the stolen computers are desktop computers means their removal was far more difficult than the removal of laptop computers, suggesting that the PII/PHI contained on the desktops was the target of the theft.

64. In the aftermath of the Data Breach, Advocate admitted it is "taking aggressive steps to reduce the possibility of this happening again, including the addition of 24/7 security personnel at this facility as well as accelerated deployment of enhanced technical safeguards," none of which are thus believed to have been in place at the time of the Data Breach.[12]

65. Advocate's wrongful actions and inaction—to wit, failing to protect Plaintiffs' and Class Members' PII/PHI with which it was entrusted—directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' unencrypted PII/PHI without their knowledge, authorization, and consent. As a further direct and proximate result of Advocate's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class Members have suffered, and will continue to suffer, economic damages and other actual

[12] "Advocate Medical Group Notifies Patients, Offers Protection Following Office Burglary," Advocate Health Care Press Release, available at http://www.advocatehealth.com/body_full.cfm?id=12&action=detail&ref=293 (last visited Dec. 4, 2013).

harm including, without limitation: (i) the untimely and inadequate notification of the Data Breach; (ii) improper disclosure of their PII/PHI; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under FCRA—for which they are entitled to compensation.

66. Notwithstanding Advocate's wrongful actions and inaction and the resulting Data Breach, Advocate has offered a mere one year of credit monitoring services, which is insufficient given the trove of unencrypted PII/PHI that was taken and disseminated to the world and the manipulation and machinations of cyber criminals.

67. As a result of Advocate's failure to properly safeguard and protect Plaintiffs' and Class Members' PII/PHI, including, *inter alia*, failing to secure the stolen desktop computers, failing to encrypt their PII/PHI, and violating standard industry practices and protocols for protecting PII/PHI, Plaintiffs' and Class Members' privacy has been (and will continue to be) invaded and their rights violated. Their compromised PII/PHI was private and sensitive in nature and was left inadequately protected and unencrypted by Advocate. Advocate's wrongful actions and inaction and the resulting Data Breach have placed Plaintiffs and Class Members at an imminent, immediate, and continuing increased risk of harm from identity theft, identity fraud, and medical fraud.

68. Adding to the culpability and willfulness, recklessness, and/or negligence of Advocate's conduct and its violation of numerous industry standards and HIPPA, is the fact that

approximately 94% of all healthcare organizations in the U.S. have suffered data breaches in the last two (2) years.[13] This is publicly available knowledge that should have been known to Advocate and caused it to provide adequate security and protection for Plaintiffs' and Class Members' PII/PHI.

69. Identity theft occurs when a person's PII, such as the person's name, e-mail address, address, Social Security number, billing and shipping addresses, phone number and credit card information is used or attempted to be used without his or her permission to commit fraud or other crimes.[14]

70. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[15] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute [PII]."[16]

71. The FTC estimates that the identities of as many as 9 million Americans are stolen each year. *Id.*

---

[13] "Ponemon Study Reveals Ninety-Four Percent of Hospitals Surveyed Suffered Data Breaches," (Dec. 6, 2013), available at http://www2.idexpertscorp.com/press/ninety-four-percent-of-hospitals-surveyed-suffered-data-breaches/ (last visited Dec. 6, 2014).

[14] *See* http://www.consumer.ftc.gov/features/feature-0014-identity-theft (last visited Dec. 4, 2013).

[15] *Protecting Consumer Privacy in an Era of Rapid Change* FTC Report (March 2012), available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (last visited Dec. 4, 2013).

[16] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, *Preliminary FTC Staff Report*, 35–38 (Dec. 2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (last visited Dec. 4, 2013); *Comment of Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11–12.

72. As a direct and proximate result of Advocate's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class Members will now be required to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, placing "freezes" and "alerts" with the credit reporting agencies, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity. Because Plaintiffs' and Class Members' Social Security numbers were stolen and compromised, as well as their medical information, they also now face a significantly heightened risk of identity theft, identity fraud, and medical fraud.

73. According to the FTC, identity theft is serious. "Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest."[17]

74. Theft of medical information, such as that included in the Data Breach here, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[18]

75. Identity thieves also use Social Security numbers to commit other types of fraud. The GAO found that identity thieves use PII/PHI to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging"

[17] *See* Federal Trade Commission, *Signs of Identity Theft*, http://www.consumer.ftc.gov/articles/0271-signs-identity-theft (last visited Dec. 4, 2013).

[18] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Dec. 4, 2013).

because it may take some time for the victim to become aware of the theft, while in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PII/PHI, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future.

76. Identity thieves also use Social Security numbers to obtain false identification cards, obtain government benefits in the victim's name, commit crimes, and file fraudulent tax returns on the victim's behalf to obtain fraudulent tax refunds. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments, and obtain medical services in the victim's name. Identity thieves also have been known to give a victim's personal information to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

77. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently, as well as show that he has done all he can to fix the problems resulting from the misuse.[19] Thus, a person whose PII/PHI has been stolen cannot obtain a new Social Security number until the damage has already been done.

78. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a

[19]*See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327, available at http://www.ssa.gov/pubs/10064.html (last visited Dec. 4, 2013).

fresh start. For some victims of identity theft, a new number may actually create new problems. Because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

79. As a direct and proximate result of Advocate's wrongful actions and inaction and the resulting Data Breach, the thieves and/or their customers now have Plaintiffs' and Class Members' PII/PHI. As such, Plaintiffs and Class Members have been deprived of the value of their PII/PHI.[20]

80. Plaintiffs' and Class Members' PII/PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for a number of years.[21] Identity thieves and other cyber criminals openly post stolen credit card numbers, Social Security numbers, and other personal financial information on various Internet websites, thereby making the information publicly available. In one study, researchers found hundreds of websites displaying stolen personal financial information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism—the "Safe Browsing list." The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not

[20] *See, e.g.*, John T. Soma, J. Zachary Courson, John Cadkin, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted); ABC News Report, http://abcnews.go.com/Health/medical-records-private-abc-news-investigation/story?id=17228986&page=2#.UGRgtq7yBR4 (last visited Dec. 4, 2013).

[21] Companies, in fact, also recognize PII/PHI as an extremely valuable commodity akin to a form of personal property. *See* T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

underground at all. In fact, it's very "in your face."[22]

81. It is reported that "medical records hold an average black market value of $50 per record."[23]

82. The Data Breach was a direct and proximate result of Advocate's failure to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect Plaintiffs' and Class Members' PII/PHI from unauthorized access, use, and disclosure, as required by various state and federal regulations and industry practices, as well as common law duties.

83. Advocate flagrantly disregarded and violated Plaintiffs' and Class Members' privacy rights, and materially harmed them in the process, by not obtaining Plaintiffs' and Class Members' prior written consent to disclose their PII/PHI to any other person—as required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and other pertinent laws, regulations, industry standards and internal company standards.

84. Advocate flagrantly disregarded and violated Plaintiffs' and Class Members' privacy rights, and materially harmed them in the process, by failing to establish and implement appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII/PHI to protect against anticipated threats to the security or integrity of such information. Advocate's security deficiencies allowed unauthorized individuals to access, remove from its premises, transport, disclose, and compromise the PII/PHI of millions of individuals—including Plaintiffs and Class Members.

---

[22] StopTheHacker, *The "Underground Credit Card Blackmarket*, available at http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/ (last visited Dec. 4, 2013).

[23] Pamela Louis Dolan, "Health Data Breaches Usually Aren't Accidents Anymore," (July 29, 2013), available at http://www.amednews.com/article/20130729/business/130729953/4/ (last visited Dec. 4, 2013).

85. Advocate's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII/PHI without their knowledge, authorization, and consent. As a direct and proximate result of Advocate's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class Members have incurred (and will continue to incur) economic damages and other harm in the form of, *inter alia*: (i) the untimely and inadequate notification of the Data Breach; (ii) improper disclosure of their PII/PHI; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under FCRA—for which they are entitled to compensation.

CLASS ACTION ALLEGATIONS

86. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this class action as a national class action on behalf of themselves and the following Class of similarly situated individuals:

> All persons whose personal identifying information (PII) and personal health information (PHI) were contained on the computers stolen from the Advocate Medical Group administrative offices at 205 West Touhy, Park Ridge, Illinois 60068, on July 15, 2013.

Excluded from the Class are (i) Advocate owners, officers, directors, employees, agents, and representatives and its parent entities, subsidiaries, affiliates, successors, and assigns; and (ii) the Court, Court personnel, and members of their immediate families.

87. The putative Class comprises over four million persons, making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

88. The rights of each Class Member were violated in a virtually identical manner as a result of Advocate's willful, reckless, and/or negligent actions and inaction.

89. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a) Whether Advocate violated FCRA by failing to properly secure Plaintiffs' and Class Members' PII/PHI;

b) Whether Advocate violated FCRA by failing to encrypt Plaintiffs' and Class Members' PII/PHI in accordance with federal standards;

c) Whether Advocate willfully, recklessly, and/or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class Members' PII/PHI;

d) Whether Advocate was negligent in storing Plaintiffs' and Class Members' PII/PHI;

e) Whether Advocate owed a duty to Plaintiffs and Class Members to exercise reasonable care in protecting and securing their PII/PHI;

f) Whether Advocate breached its duty to exercise reasonable care in protecting and securing Plaintiffs' and Class Members' PII/PHI;

g) Whether Advocate was negligent in failing to secure Plaintiffs' and Class Members' PII/PHI;

h) Whether by publicly disclosing Plaintiffs' and Class Members' PII/PHI without authorization, Advocate invaded Plaintiffs' and Class Members' privacy;

i) Whether Plaintiffs and Class Members sustained damages as a result of Advocate's failure to secure and protect their PII/PHI; and

j) Whether Advocate violated federal and state laws by failing to timely notify Plaintiffs and Class Members on an individual basis about the theft and dissemination of their PII/PHI.

90. Plaintiffs' claims are typical of Class Members' claims in that Plaintiffs' claims and Class Members' claims all arise from Advocate's failure to properly safeguard and protect Plaintiffs' and Class Members' PII/PHI and the resulting Data Breach.

91. Plaintiffs and their counsel will fairly and adequately represent the interests of Class Members. Plaintiffs have no interests antagonistic to, or in conflict with, Class Members' interests. Plaintiffs' attorneys are highly experienced in the prosecution of consumer class actions and data breach class actions, and intend to vigorously prosecute this action on behalf of Plaintiffs and Class Members. Their work in this litigation to date confirms that ability and effort.

92. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiffs' and Class Members' claims. Plaintiffs and Class Members have been irreparably harmed as a result of Advocate's wrongful actions and inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Advocate's failure to secure and protect Plaintiffs' and Class Members' PII/PHI.

93. Class certification, therefore, is appropriate pursuant to FED. R. CIV. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

94. Class certification also is appropriate pursuant to FED. R. CIV. P. 23(b)(2) because Advocate has acted or refused to act on grounds generally applicable to the Class, thereby making final injunctive relief appropriate with respect to the Class as a whole.

95. Class certification also is appropriate because the expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights.

CLAIMS FOR RELIEF

COUNT I

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

96. The preceding paragraphs are incorporated by reference, as if fully set forth herein.

97. In enacting FCRA, Congress made several findings, including that "*[t]here is a need to insure* that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and *a respect for the consumer's right to privacy*." 15 U.S.C. § 1681(4) (emphasis added).

98. FCRA requires consumer reporting agencies to *adopt and maintain reasonable procedures* for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner fair and equitable to consumers *while maintaining the confidentiality*, accuracy, relevancy, and proper utilization of such information. 15 U.S.C. § 1681(b).

99. FCRA defines a "consumer reporting agency" as:

> Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

100. FCRA defines a "consumer report" as:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b).

15 U.S.C. § 1681a(d)(1).

101. FCRA defines "medical information" as:

> [I]nformation or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to—(A) the past, present, or future physical, mental, or behavioral health or condition of an individual; (B) the provision of health care to an individual; or (C) the payment for the provision of health care to an individual.

15 U.S.C. § 1681a(i).

102. FCRA specifically protects medical information, restricting its dissemination to limited instances. *See, e.g.*, 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681c(a)(6).

103. Plaintiffs' PII/PHI constitute Consumer Reports because the information bears on their character, general reputation, personal characteristics, and/or mode of living, and is used and collected by Advocate for the purpose of, *inter alia*, establishing Plaintiffs' eligibility for health insurance coverage, including for the payment of health care services to doctors that are members of Advocate.

104. Advocate is a Consumer Reporting Agency, as defined under FCRA, because on a cooperative nonprofit basis and/or for monetary fees, Advocate regularly engages, in whole or in part, in the practice of assembling information on consumers for the purpose of furnishing

Consumer Reports to third parties and/or uses interstate commerce for the purpose of preparing and/or furnishing Consumer Reports.

105. As a Consumer Reporting Agency, Advocate was (and continues to be) required to adopt and maintain procedures designed to protect and limit the dissemination of consumer credit, personnel, insurance and other information (such as Plaintiffs' and Class Members' PII/PHI) in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. *See* 15 U.S.C. § 1681(b).

106. Advocate, however, violated FCRA by failing to adopt and maintain such protective procedures which, in turn, directly and proximately resulted in the theft of the unsecured and unmonitored desktop computers containing Plaintiffs' and Class Members' unencrypted PII/PHI and its wrongful dissemination into the public domain. In addition to properly securing and monitoring the stolen desktop computers and encrypting Plaintiffs' and Class Members' PII/PHI on the computers, Advocate could have (and should have):

a) Conducted periodic risk assessments and gap analysis relating to privacy and information security-related policies, processes and procedures. A comprehensive risk analysis would have identified the (i) physical vulnerability of Advocate's locations, (ii) administrative vulnerabilities associated with storing over four million patient records on four desktop computers, and (iii) technical vulnerabilities, including the need to restrict unauthorized access and encrypt at-risk data.

b) Developed privacy and information security related performance and activity metrics, such as the performance of ongoing compliance reviews, physical walkthroughs (roundings), hotline and complaint management—and ensure that these metrics were an integral part of Advocate's corporate governance program.

c) Taken measures to monitor and secure the room and areas where the desktop computers containing the PII/PHI were stored, maintained, and used, or taken measures to insure that no PII/PHI was stored on unencrypted electronic devices.

On information and belief, Advocate took none of these proactive actions to secure the stolen desktop computers and safeguard and protect Plaintiffs' and Class Members' PII/PHI and failed to place itself in a position to immediately notify Plaintiffs and Class Members about the Data Breach.

107. Plaintiffs' and Class Members' PII/PHI, in whole or in part, constitutes medical information as defined by FCRA. Advocate violated FCRA by failing to specifically protect and limit the dissemination of Plaintiffs' and Class Members' PII/PHI (*i.e.*, their medical information) into the public domain.

108. As a direct and proximate result of Advocate's willful and/or reckless violations of FCRA, and the resulting Data Breach, as described above, Plaintiffs' and Class Members' unencrypted PII/PHI was taken and made accessible to unauthorized third parties in the public domain.

109. As a direct and proximate result of Advocate's willful and/or reckless violations of FCRA, and the resulting Data Breach, as described above, Plaintiffs and Class Members were (and continue to be) damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, other out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

110. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages including, *inter alia*, (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (iv) anxiety and emotional distress; and (v)

statutory damages of not less than $100, and not more than $1000, each, as well as attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681n(a).

COUNT II

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

111. The factual statements and allegations in paragraphs 1–107 of this Amended Class Action Complaint are incorporated by reference, as if fully set forth herein.

112. In the alternative, and as described above, Advocate negligently violated FCRA by failing to adopt and maintain procedures designed to protect and limit the dissemination of Plaintiffs' and Class Members' PII/PHI for the permissible purposes outlined by FCRA which, in turn, directly and proximately resulted in the theft of the unsecured and unmonitored desktop computers containing Plaintiffs' and Class Members' unencrypted PII/PHI and its wrongful dissemination into the public domain. In addition to properly securing and monitoring the stolen desktop computers and encrypting Plaintiffs' and Class Members' PII/PHI on the computers, Advocate could have (and should have):

a) Conducted periodic risk assessments and gap analysis relating to privacy and information security-related policies, processes and procedures. A comprehensive risk analysis would have identified the (i) physical vulnerability of Advocate's locations, (ii) administrative vulnerabilities associated with storing over four million patient records on four desktop computers, and (iii) technical vulnerabilities, including the need to restrict unauthorized access and encrypt at-risk data.

b) Developed privacy and information security related performance and activity metrics, such as the performance of ongoing compliance reviews, physical walkthroughs (roundings), hotline and complaint management—and ensure that these metrics were an integral part of Advocate's corporate governance program.

c) Taken measures to monitor and secure the room and areas where the desktop computers containing the PII/PHI were stored, maintained, and used, or taken measures to insure that no PII/PHI was stored on unencrypted electronic devices.

On information and belief, Advocate took none of these proactive actions to secure and protect Plaintiffs' and Class Members' PII/PHI and failed to place itself in a position to immediately notify Plaintiffs and Class Members about the Data Breach.

113. It was reasonably foreseeable that Advocate's failure to implement and maintain procedures to safeguard and protect Plaintiffs' and Class Members' PII/PHI would result in an unauthorized third party gaining access to their PII/PHI for no permissible purpose under FCRA.

114. As a direct and proximate result of Advocate's negligent violations of FCRA, and the resulting Data Breach, as described above, Plaintiffs' and Class Members' PII/PHI was stolen and made accessible to unauthorized third parties in the public domain.

115. As a direct and proximate result of Advocate's negligent violations of FCRA, and the resulting Data Breach, as described above, Plaintiffs and the Class Members were (and continue to be) damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, other out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

116. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages, including, *inter alia*: (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (iv) anxiety and emotional distress; and (viii) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681o(a).

COUNT III

NEGLIGENCE

117. The factual statements and allegations in paragraphs 1–116 of this Complaint are incorporated by reference as if fully set forth herein.

118. Advocate had a duty to exercise reasonable care and caution in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

119. Advocate violated its duty by failing to exercise reasonable care and caution and safeguard and protect Plaintiffs' and Class Members' PII/PHI (as set forth in detail above).

120. It was reasonably foreseeable that Advocate's failure to exercise reasonable care and caution in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI would result in an unauthorized third party gaining access to such information for no lawful purpose.

121. Plaintiffs and the Class Members were (and continue to be) damaged as a direct and proximate result of Advocate's failure to secure and protect their PII/PHI in the form of, *inter alia*, (i) improper disclosure of their PII/PHI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (vi) anxiety and emotional distress— for which they are entitled to compensation.

122. Advocate's wrongful actions and inaction (as described above) constituted negligence at common law.

COUNT IV

INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

123. The factual statements and allegations in paragraphs 1–95 of this Complaint are incorporated herein by reference.

124. Advocate's failure to secure and protect Plaintiffs' and Class Members' PII/PHI directly resulted in the public disclosure of such private information.

125. Dissemination of Plaintiffs' and Class Members' PII/PHI is not of a legitimate public concern; publicity of their PII/PHI would be, is and will continue to be offensive to reasonable people.

126. Plaintiffs and the Class Members were (and continue to be) damaged as a direct and proximate result of Advocate's invasion of their privacy by publicly disclosing their private facts (*i.e.*, their PII/PHI) in the form of, *inter alia*: (i) improper disclosure of their PII/PHI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (vi) anxiety and emotional distress— for which they are entitled to compensation. At the very least, Plaintiffs and the Class Members are entitled to nominal damages.

127. Advocate's wrongful actions and inaction (as described above) constituted (and continue to constitute) an ongoing invasion of Plaintiffs' and Class Members' privacy by publicly disclosing their private facts (*i.e.*, their PII/PHI).

RELIEF REQUESTED

128. The preceding factual statements and allegations are incorporated herein by reference.

129. **DAMAGES.** As a direct and proximate result of Advocate's wrongful actions and inaction, and the resulting Data Breach (as described above), Plaintiffs and Class Members suffered (and continue to suffer) economic damages and other harm in the form of, *inter alia*: (i) the untimely and inadequate notification of the Data Breach; (ii) improper disclosure of their PII/PHI; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under FCRA—for which they are entitled to compensation. Plaintiffs and Class Members also are entitled to recover statutory damages and/or nominal damages. Plaintiffs' and Class Members' damages were foreseeable by Advocate and exceed the minimum jurisdictional limits of this Court.

130. **EXEMPLARY DAMAGES.** Plaintiffs and Class Members also are entitled to exemplary damages as punishment and to deter such wrongful conduct in the future.

131. **INJUNCTIVE RELIEF.** Plaintiffs and Class Members also are entitled to injunctive relief in the form of, without limitation, requiring Advocate to, *inter alia,* (i) immediately disclose to Plaintiffs and Class Members the precise nature and extent of their PII/PHI contained on the stolen desktop computers, (ii) make prompt and detailed disclosure to all past, present and future patients affected by any future data breaches of their PII/PHI, (iii) immediately encrypt the

PII/PHI of its past, present, and future patients, (iv) implement the above-referenced proactive policies and procedures in order to secure and protect its patients' PII/PHI and be in a position to immediately notify them about any data breaches, (v) submit to periodic compliance audits by a third party regarding the implementation of and compliance with such policies and procedures, and (vi) submit to periodic compliance audits by a third party regarding the security of its patients' PII/PHI within its possession, custody and control.

132. **ATTORNEYS' FEES, LITIGATION EXPENSES AND COSTS.** Plaintiffs and Class Members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action pursuant to, *inter alia*, 15 U.S.C. §§ 1681n(a); o(a).

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, respectfully request that (i) Advocate be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiffs be designated the Class Representatives, and (iv) Plaintiffs' counsel be appointed as Class Counsel. Plaintiffs, on behalf of themselves and Class Members, further request that upon final trial or hearing, judgment be awarded against Advocate, in favor of Plaintiffs and the Class Members, for:

(i) actual damages, consequential damages, FCRA statutory damages, and/or nominal damages (as described above) in an amount to be determined by the trier of fact;

(ii) exemplary damages:

(iii) injunctive relief as set forth above;

(iv) pre- and post-judgment interest at the highest applicable legal rates;

(v) attorneys' fees and litigation expenses incurred through trial and any appeals;

(vi) costs of suit; and

(vii) such other and further relief that the Court deems just and proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and all others similarly situated, respectfully demand a trial by jury on all of the claims and causes of action so triable.

December 6, 2013

Respectfully submitted,

/s/ Ben Barnow
Ben Barnow
Sharon Harris
Blake A. Strautins
BARNOW AND ASSOCIATES, P.C.
One N. LaSalle Street, Ste. 4600
Chicago, IL 60602
Telephone: (312) 621-2000
Facsimile: (312) 641-5504
Email: b.barnow@barnowlaw.com
Email: s.harris@barnowlaw.com
Email: b.strautins@barnowlaw.com

Richard L. Coffman (*admitted pro hac vice*)
THE COFFMAN LAW FIRM
First City Building
505 Orleans St., Ste. 505
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
Email: rcoffman@coffmanlawfirm.com

Aron D. Robinson
LAW OFFICE OF ARON D. ROBINSON
180 West Washington St., Suite 700
Chicago, IL 60602
Telephone: (312) 857-9050
Email: Adroblaw@aol.com

Interim Class Counsel

Kevin Rogers
LAW OFFICES OF KEVIN ROGERS
307 N. Michigan Ave, Suite 305
Chicago, IL 60601
Telephone: (312) 332-1188
Facsimile: (312) 332-0192
Email: Kevin@kevinrogerslaw.com

Additional Plaintiffs' Counsel

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Amended Class Action Complaint was served on all counsel of record via the Court's ECF filing system.

Dated: December 6, 2013

/s/ Ben Barnow
Ben Barnow

One of Interim Class Counsel